ABSTRACT

Content stored in a non-volatile storage device is protected from unauthorized modification and/or access. The device is configured as one or more regions, where one or more of the regions implements one or more content protection schemes. The current version of the contents stored in a region is compared to a previously stored valid version to determine if the current version has been modified without authorization. A region may be protected by use of an integrity metric (*e.g.*, checksum, bit mask, and/or cyclic redundancy check value). The methodology may be implemented during the start up sequence of a computer system to protect the basic I/O system (BIOS) from unauthorized modification.